Security Enhanced Cooperative Game Theory for Mobile Ad-Hoc Network

Bondu Madhavi[1], D.Murali[2]
[1]PG Student, QUBA College of engineering and technology
[2]Associate Professor, QUBA College of engineering and technology

Abstract: Mobile Ad-hoc Networks (MANETs) are decentralized, self-configuring wireless systems where nodes cooperate to enable communication in the absence of fixed infrastructure. However, the dynamic topology, limited resources, and vulnerability to malicious behavior pose significant challenges to secure and reliable data transmission. Traditional security mechanisms often rely on cryptography or trust management, which may not be sufficient in highly dynamic environments. To address these issues, this work proposes a Security-Enhanced Cooperative Game Theory (SE-CGT) framework for MANETs. The framework models node interactions as cooperative games, where nodes form coalitions to maximize overall network utility while ensuring fairness, reliability, and resistance to selfish or malicious behavior. Security is incorporated by integrating reputation-based trust evaluation and incentive-compatible mechanisms, ensuring that cooperative nodes are rewarded and malicious nodes are penalized or excluded. Simulation studies demonstrate that SE-CGT improves packet delivery ratio, reduces routing overhead, and enhances network lifetime compared to existing game-theoretic and trust-based approaches. This research highlights the potential of combining cooperative game theory with security enhancements to achieve robust, scalable, and energy-efficient communication in MANETs.

Index Terms— Mobile Ad-hoc Networks (MANETs), Cooperative Game Theory, Security Enhancement, Trust Management, Incentive Mechanisms, Secure Routing

1. INTRODUCTION

1.1 Introduction for Communication Systems

Communication is the process by which two or more people exchange ideas, facts, feelings, or impressions in ways that each gains a common understanding of the meaning, intent, and use of messages.

The term "communication" stems from the Latin word "communism" - meaning common. Thus, communication is a conscious attempt to share information, ideas, attitudes, and the like with others.

1.2 Need for Communication Systems

In short, it is the act of getting a sender of the message and a receiver of the message tuned together for a particular message, or a series of messages. For two or more people to engage in a common, co-operative effort, they must be able to communicate with each other. Thus, good communication consists of creating understanding of the message. In computerized technology, we need to transfer the data from one another without any problem like security and quality. To improve the communication in mobile adhoc network we need to test our proposed method is working well or not by using system modeling. System modeling refers to an act of representing an actual system in a simply way.

System modeling is extremely important in system design and development, since it gives an idea of how the system would perform if actually implemented.

1.3 What does security mean:

Ability for [two] nodes to effectively communicate even in the presence of active adversaries in the network

Ability to find routes

Availability of service

If an “honest” path exists

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network

administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority.

The networks are computer networks, both public and private, that are used every day to conduct transactions and communications among businesses, government agencies and individuals. The networks are comprised of "nodes", which are "client" terminals (individual user PCs), and one or more "servers" and/or "host" computers. They are linked by communication systems, some of which might be private, such as within a company and others which might be open to public access.

The obvious example of a network system that is open to public access is the Internet, but many private networks also utilize publicly-accessible communications. Today, most companies' host computers can be accessed by their employees whether in their offices over a private communications network, or from their homes or hotel rooms while on the road through normal telephone lines.

Network security involves all activities that organizations, enterprises, and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them.

1.4 Objective:

In our scheme, the address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected using a reverse tracing technique. Our ultimate goal is to achieve the security without relying on key management in MANET.

1.5 Literature Survey:

Kejun Liu, Jing Deng, Pramod K. Varshney and Kashyap Balakrishnan, “Based Approach for the Detection of Routing Misbehavior in MANETS”. It presents author proposed the 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehavior and to mitigate their diverse effect. The main idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. Compared with other approaches to combat the problem, such as the overhearing technique, the 2ACK scheme overcomes several problems including ambiguous collisions, receiver collisions, and limited transmission powers. The 2ACK scheme can be used as an add-on technique to routing protocols such as DSR in MANETs. But, the knowledge of topology of the 2-hop neighborhood may be used. In addition, the 2ACK scheme can only work in managed MANETs (as compared to open MANETs).

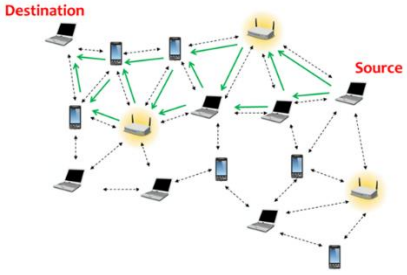


Fig no:1.1 Disaster relief operations

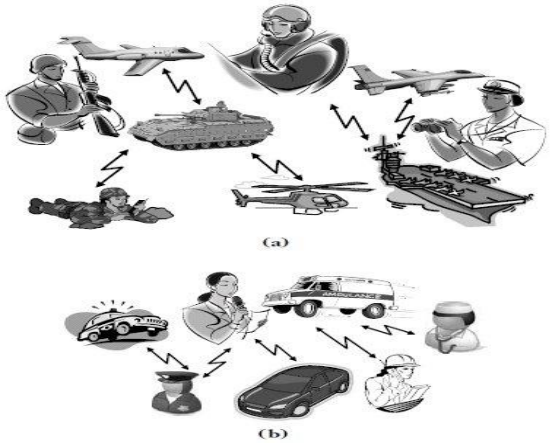


Fig no:1.2 Military or police exercises

1.7 Disadvantage

AODV doesn’t allow handling unidirectional links. Multiple Route Reply packets in response to a single Route Request packet can lead to heavy control overhead. Periodic beaconing leads to unnecessary bandwidth consumption.

1.8 Applications

Some of the applications of MANETs are

- Military or police exercises.
- Disaster relief operations.
- Mine site operations.

II WIRELESS NETWORKS AND ROUTING PROTOCOLS

2.1 Introduction to routing protocols

DSR includes source routes in packet headers. Resulting large headers can sometimes degrade performance-particularly when data contents of a packet are small, AODV attempts to improve on DSR by maintaining routing tables at the nodes, so that data packets do not have to contain routes. AODV retains the desirable feature of DSR that routes are maintained only between nodes which need to communicate. Route Requests (RREQ) are forwarded in a manner similar to DSR. When a node re-broadcasts a Route Request, it sets up a reverse path pointing towards the source-AODV assumes symmetric (bi-directional) links.

When the intended destination receives a Route Request, it replies by sending a Route Reply (RREP).Route Reply travels along the reverse path set-up when Route Request is forwarded. Route Request (RREQ) includes the last known sequence number for the destination. An intermediate node may also send a Route Reply (RREP) provided that it knows a more recent path than the one previously known to sender. Intermediate nodes that forward the RREP, also record the next hop to destination. A routing table entry maintaining a reverse path is purged after a timeout interval. A routing table entry maintaining a forward path is purged if not used for a active_route_timeout interval.

A neighbor of node X is considered active for a routing table entry if the neighbor sent a packet within active_route_timeout interval which was forwarded using that entry. Neighboring nodes periodically exchange hello message. When the next hop link in a routing table entry breaks, all active neighbors are informed. Link failures are propagated by means of Route Error (RERR) messages, which also update destination sequence numbers.

When node X is unable to forward packet P (from node S to node D) on link (X, Y), it generates a RERR message. Node X increments the destination sequence number for D cached at node X. The incremented sequence number N is included in the RERR.

2.2 Different types of Wireless networks

Wireless networks provide unprecedented freedom and mobility for a growing number of laptop and PDA users who no longer need wires to stay connected with their workplace and the Internet. Ironically, the very devices that provide wireless service to these clients need lots of wiring themselves to connect to private networks and the Internet. This white paper presents a viable alternative to all those wires - the wireless mesh network.

III MANAGEMENT INFRASTRUCTURE

3.1 Key Management Method

There are two complementary classes of approaches that can safeguard tactical MANETs: prevention-based and detection based approaches.

3.1.1Prevention Based

One issue of these prevention-based approaches is that a centralized key management infrastructure is needed, which may not be realistic in distributed networks such as MANETs. In addition, a centralized infrastructure will be the main target of rivals in battlefields. If the infrastructure is destroyed, then the whole network may be paralyzed.

3.1.2Detection Based

Serving as the second wall of protection, detection-based approaches can effectively help identify malicious activities. Although some excellent work has been done on detection based approaches based on trust in MANETs, observation in most approaches is only used to assess the reliability of nodes, which are not in the range of the observer node. Therefore, inaccurate trust values may be derived. Most of existing works on applying game theories to security only consider two players in the security game model: an attacker and a defender. While this assumption may be valid for a network with centralized administration, it is not realistic in MANETs, where centralized administration is not available

3.2 Trust Management Method

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks.

Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over

time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes them selves, i.e., routing functionality will be incorporated into mobile nodes. Many research works have focused on the security of MANETs.

Most of them deal with prevention and detection approaches to combat individual misbehaving nodes. In this regard, the effectiveness of these approaches becomes weak when multiple malicious nodes collude together to initiate a collaborative attack, which may result to more devastating damages to the network. A mobile ad hoc network is a collection of wireless nodes that can dynamically be set up anywhere and anytime without using any pre-existing network infrastructure.

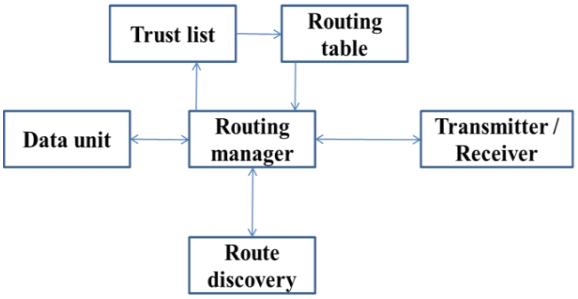


Fig no:3.1 Block diagram of data Flow

We have divided our project into small four modules and sub modules to improve our work process.

1) Route Discovery
a. Data transmission
b. Basic Malicious attack
2) Direct Observation
a. Ack based observation
b. Data based observation
3) Indirect Observation
a. Opinion Req/Rep sharing
4) Coop communication

3.3 Route Discovery

If node has the data without route then the node has to wait until forming the route to destination. To check the route, the node will use the Modified AODV routing protocol by flooding the Req/Rep message, the route will be formed b/w source and destination. If route is found then the data can be transfer to the destination. Number of attacks is there against MANET's. In our project we are going to prevent good nodes from the Fake reply with gray hole attack nodes.

In this module we are creating the model of gray hole attack node. The node which is going to forward some of the data to destination and remaining data will be lost is called gray hole attack.

IV. SIMULATION RESULTS

4.1 Simulation Approach

Simulation is a process of designing a model of a real system and conducting experiments with this model for the purpose of understanding the behavior of the system and/or evaluating various strategies for the operation of the system.

Simulation is widely-used in system modeling for applications ranging from engineering research, business analysis, manufacturing planning, and biological science experimentation, just to name a few. Compared to analytical modeling, simulation usually requires less abstraction in the model (i.e., fewer simplifying assumptions) since almost every possible detail of the specifications of the system can be put into the simulation model to best describe the actual system. When the system is rather large and complex, a straightforward mathematical formulation may not be feasible. In this case, the simulation approach is usually preferred to the analytical approach.

In common with analytical modeling, simulation modeling may leave out some details, since too many details may result in an unmanageable simulation and substantial computation effort. It is important to carefully consider a measure under consideration and not to include irrelevant detail into the simulation.

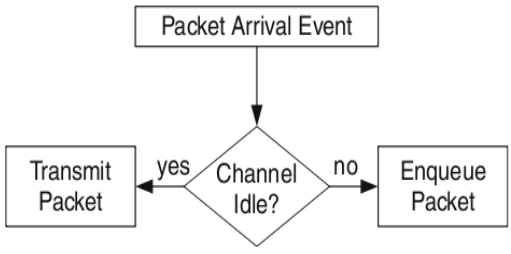


Fig no:4.1 Packet arrival event

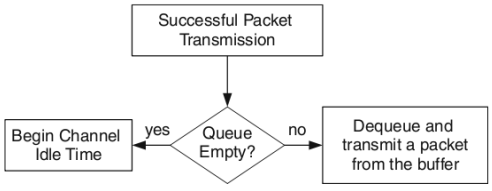
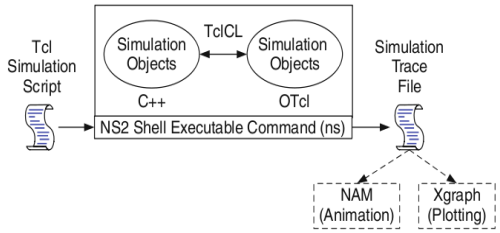


Fig no:4.2 Succesfull packet transmission

4.2 Introduction about NS2:

Network Simulator (Version 2), widely known as NS2, is simply an event driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done using NS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviors.

Due to its flexibility and modular nature, NS2 has gained constant popularity in the networking research community since its birth in 1989.



4.2.1 Installation of Ns2:

After completing the installation of ubuntu 10.04, update all the things in that. How to update means Goto the top menu, system-Administration-update manager

Step: 1

-Open the terminal. For this Goto Application-Accessories-Terminal (or press Ctrl+alt+T)

-Then paste the following command

sudo apt-get install build-essential autoconf automake libxmu-dev gcc-4.3

Step: 2

Then u need to some files. So For this, open the Ns-allinone2.34 folder on the desktop, in that open folder OTCL1.13. In that folder, u need to modify the following files.

1. Modify Makefile.in file

In this file, u need to replace CC= @CC@

With CC= gcc-4.3

To replace this press ctrl+H.

Then save the document.

2. Modify configure.in and configure files.

In these two files u need to modify. Means u need to replace ld -shared with gcc –shared. For replacing ctrl+H then one dialog box will come. Then save the document.

Step: 3

Open the ns-allinone2.34 folder which is present on the desktop,

Then press ctrl+L. Then copy the path on the address bar.

Step: 4

Then open Terminal and do the following.

Type $cd “paste the path here” without quotes and press enter.

Then

Type $./install

Then wait for some time, finally if successfully installed, it will display a message as “for Related Posts”. Otherwise some problems might have occurred.

Step: 5

Then execute the following command in the Terminal

$ gedit ~/.bashrc

Then one document will be opened automatically.

Then delete all the content in that document and paste the following code in it.

4.3 Simulation Result:

We have implemented the security system, which is based on the ACK

Here we are assuming 9 nodes for the implementation of the all the scenarios

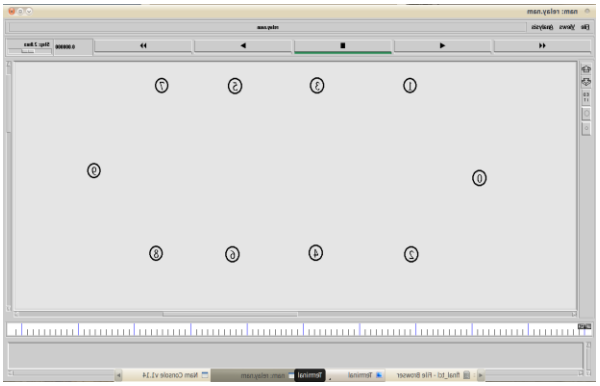


Fig.4.3 simplified network scenario with source and destination

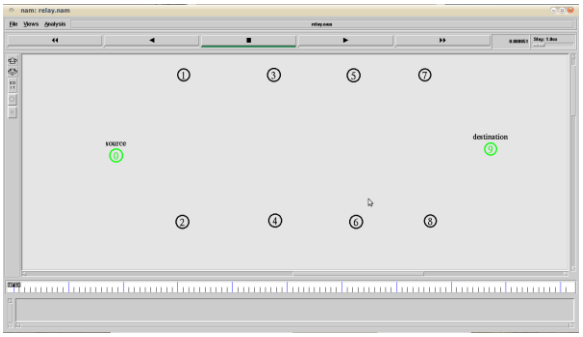


Fig.4.4 source node and destination node

V. CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

In this project, a Security-Enhanced Cooperative Game Theory approach has been explored for improving the reliability and security of Mobile Ad-hoc Networks (MANETs). We initially implemented an acknowledgement-based verification process to detect malicious nodes. This mechanism allowed nodes to cross-check the forwarding behavior of their neighbors and identify misbehavior based on missing acknowledgements. Although effective in basic scenarios, the ACK-based scheme alone was found to be insufficient for making a final decision regarding the trustworthiness of nodes, since packet drops could also occur due to network congestion, collisions, or energy depletion rather than intentional misbehavior.

To overcome these limitations, a cooperative trust verification process was incorporated. By allowing multiple nodes to participate in the evaluation of a given node's behavior, a more accurate and reliable decision was achieved. This cooperation-based trust mechanism ensures that malicious nodes can be effectively detected and isolated, thereby reducing the impact of selfish or adversarial behavior. The combination of acknowledgement monitoring and cooperative trust evaluation significantly enhances the overall security, packet delivery ratio, and robustness of MANET communications.

5.2 Future Scope

While the proposed system successfully improves malicious node detection through cooperative trust management, there is still ample scope for enhancement. Future work can explore the following directions:

Energy-Aware Routing: Instead of relying solely on cooperation and trust mechanisms, the residual energy levels of nodes can be incorporated into the decision-making process. By selecting routes with nodes that have higher energy reserves, the stability of the network can be improved and the risk of path failure due to node exhaustion can be minimized.

REFERENCE

[1] An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs----> Kejun Liu, Jing Deng, Pramod K. Varshney and Kashyap Balakrishnan.

[2] "Mitigating routing misbehavior in mobile ad hoc networks," S. Marti, T. J. Giuli, K. Lai, and M. Baker.

[3] A Survey of Secure Wireless Ad Hoc Routing", Yi-Chun Hu, Adrian Perrig 2004 IEEE, May/June 2004.

[4] A secure On- Demand Routing Protocol for Ad Hoc Networks Yih-Chun, Adrian Perrig, David B. Johnson Ariadne, 2002.

[5] Mobile Ad Hoc Networking Working Group Charles E. Perkins, Elizabeth M. Belding-Royer, Samir R.Das, February 2003.

[6] A robust reputation system for mobile adhoc networks, S. Buchegger and J. Y. Le Boudec. July 2003.

[7] Self-Organized Public-Key Management for Mobile Ad Hoc Networks---> Srdjan Capkun, Levente Butty´ n and Jean-Pierre Hubaux.

[8] ALARM: Anonymous Location-Aided Routing in Suspicious MANETs---> Karim El Defrawy and Gene Tsudik.

[9] Identity-Based Encryption from the Weil Pairing---> Dan Boneh, Matthew Franklin.

[10] SybilGuard: Defending Against Sybil Attacks via Social Networks---> Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons, Abraham Flaxman.

[11] "Trust and Reputation Model in Peer-to-Peer Networks", Yao Wang, Julita Vassileva puts